John V. Picone III (State Bar No. 187226)
jpicone@hopkinscarley.com
Jennifer Coleman (State Bar No. 213210)
jcoleman@hopkinscarley.com
C. Gideon Korrell (State Bar No. 284890)
gkorrell@hopkinscarley.com
HOPKINS & CARLEY
A Law Corporation
The Letitia Building
70 South First Street
San Jose, CA 95113-2406

mailing address:
P.O. Box 1469
San Jose, CA 95109-1469
Telephone: (408) 286-9800
Facsimile: (408) 998-4790

Attorneys for Plaintiff
PACE Anti-Piracy, Inc.

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

PACE ANTI-PIRACY, INC., a California corporation,

Plaintiff,

v.

INSIDE SECURE, a French legal entity, and INSIDE SECURE CORP., a Delaware corporation,

Defendants.

CASE NO. 5:17-cv-5860

COMPLAINT FOR PATENT INFRINGEMENT AND DEMAND FOR JURY TRIAL

Plaintiff PACE Anti-Piracy, Inc. ("PACE" or "Plaintiff"), by and through its attorneys, brings this Complaint against Inside Secure, a French legal entity ("Inside Secure FR") and Inside Secure Corp., a Delaware corporation ("Inside Secure US"), (collectively "INSIDE" or "Defendant"), and alleges as follows:

NATURE OF ACTION

1. This is an action for patent infringement arising under the patent laws of the United States, 35 U.S.C. § 1 *et seq.*, specifically including 35 U.S.C. § 271(a).

/ / /

PARTIES

2. PACE Anti-Piracy, Inc. is a California Corporation with a principal place of business at 1860 South Bascom Avenue, Campbell, California, 95008. PACE is the sole owner of the '149 Patent.

3. On information and belief, the Defendant, Inside Secure FR is, and at all times mentioned herein was, a French corporation doing business in California.

4. On information and belief, the Defendant, Inside Secure US, is a corporation organized and existing under the laws of the State of Delaware, with its principle place of business at 3031 Tisch Way, Suite 701, San Jose, California 95128, doing business in California.

5. On information and belief, on or about December 6, 2010, Inside Secure FR changed its name to its present name from its previous name of INSIDE Contactless Corporation.

6. On information and belief, on December 23, 2010, Inside Secure US changed its name to its present name from INSIDE Contactless Corporation.

7. On information and belief, Inside Secure FR and Inside Secure US are the same entity.

JURISDICTION AND VENUE

8. This action arises under the Patent Laws of the United States of America, Title 35 of the United States Code. This Court has subject matter jurisdiction over the action under 28 U.S.C. §§ 1331 and 1338.

9. This Court has personal jurisdiction over Defendant because Defendant conducts and has conducted business in the State of California, and has facilities and operations based in California and within this judicial district. Defendant uses, sells, and offers to sell infringing software products which perform methods of anti-piracy protection that infringe the '149 Patent within the United States, the State of California, and this judicial district.

10. Defendant imports and sells infringing software products to customers within the United States, the State of California, and this judicial district. Such customers include Synopsys, Inc., whose headquarters and principal place of business are in Mountain View, within this judicial district.

11. Defendant derives revenue from its sales of infringing software products within California and this judicial district. Such infringing software products continue to be sold, offered for sale, used, and imported in the United States, California, and this judicial district.

12. Venue is proper in this judicial district under 28 U.S.C. §§ 1391(b) and (c) because Defendant regularly transacts business within this judicial district and, relevant transactions and occurrences giving rise to the claims asserted herein occurred in this judicial district. Accordingly, Defendant has a continuing presence and the requisite minimum contacts with the Northern District of California, such that this venue is a fair and reasonable one.

INTRA-DISTRICT ASSIGNMENT

13. Because this action is an Intellectual Property Action identified in Civil L.R. 3-2(c), the action is to be assigned on a district-wide basis.

THE PATENT-IN-SUIT

14. On April 12, 2005, U.S. Patent No. 6,880,149 ("the '149 Patent"), entitled "Method for Runtime Code Integrity Validation Using Code Block Checksums," issued to Paul A. Cronce, a true and correct copy of which is attached hereto as Exhibit A.

15. On March 7, 2002, Mr. Cronce executed an inventor assignment, assigning to PACE the inventions disclosed in the patent application which subsequently issued as the'149 Patent.

16. On March 29, 2002, Mr. Cronce executed a declaration and power of attorney for utility patent application, declaring that he is the first and sole inventor of the subject matter claimed in the patent application which subsequently issued as the '149 Patent.

17. The '149 Patent relates to a method for code integrity validation of a software application program during program runtime using code block checksums. The inventions claimed in the '149 Patent allow, for example, an author of source code to generate and store checksum information that is unique to the author's source code executable, which can later be compared to a checksum that is generated at later time (e.g., after the executable has been distributed to customers), thereby confirming integrity. To further fortify the strength of the protection, the inventions claimed in the '149 Patent perform checksum validations over a period

of time rather than just prior to execution of the main application and the validation information is embedded throughout the executable code (the "protected software program"), making it extremely difficult to hack.

18. Previous attempts to thwart software piracy typically involved encryption schemes, digital signatures, and the use of license files of various types. In most instances, however, these protection schemes include a single point (or small number of points) of validation which, if located and neutralized/bypassed by a hacker, render the software unprotected (i.e., no longer requiring validation). In these cases, hackers may find success by simply locating these single/few points of vulnerability with a pattern-matching search program.

19. Claim 1 of the '149 patent reads:

> 1. A method for performing runtime checksum validation of a software program, the method comprising the steps of:
>
> (a) providing a software tool as well as instructions on how to modify the software program to submit to the tool, wherein executable code is generated from the modified software program that includes checksum information for the tool to use when processing the software program;
>
> (b) in response to the executable code being submitted to the tool, the tool calculates at least one checksum, embeds the checksum in the executable code in a location indicated by the checksum information, and strips the checksum information from the executable code; and
>
> (c) delivering the executable code as a protected software program, wherein during execution, the protected software application generates a new checksum and determines that the software application has been modified if the new checksum fails to match the embedded checksum.

FACTUAL BACKGROUND

20. PACE is a global leader in developing innovative cyber security, anti-piracy, and digital rights management software and hardware products for major software publishing companies. Since 1985, PACE's industry-leading software and hardware solutions have provided software publishers and distributors with tools to secure its customer's software application programs from unauthorized copying, modification, tampering, and/or distribution.

/ / /

21. INSIDE offers to sell and sells a software tool that it markets under the name "Core" which is used by its customer's to modify their software application programs to include runtime checksum validation functionality and "defend themselves from hackers, pirates, targeted malware, insider betrayal, and even hardware errors." *See, e.g.*, https://www.insidesecure.com/Products/Application-Protection/Software-Protection/Core (accessed on 9/23/2017).

22. INSIDE describes its infringing Core software tool as providing protection of application software by using techniques such as software "Obfuscation," which it purports to involve a process of "distribut[ing] hundreds and thousands of security fragments throughout [the] source code." *Id.* The method of creating, distributing, and verifying these "security fragments" by INSIDE's infringing Core software tool is covered by the '149 Patent.

23. INSIDE has no right or authority to infringe the '149 Patent.

24. INSIDE has sold and continues to sell its Core software tool that is covered by the '149 Patent to third parties within this judicial district, including, but not limited to Synopsys, Inc.

25. On information and belief, INSIDE's infringing Core software tool includes the steps of submitting a customer's modified software application program to the Core software tool for generating a modified software program with an executable that includes checksum information for the tool to use when processing the software program, the Core software tool then calculates at least one checksum, embeds it into the executable code in a location indicated by the checksum information, and then strips the checksum information from the executable code. This process of embedding the checksum creates a protected software program that, during execution, generates a new checksum which the software program uses to determine any tampering—a mismatch in the generated checksum and embedded checksum is an indication of a modification of the software.

26. In view of the foregoing, INSIDE's infringing Core software tool embodies each limitation of at least claims 1, 2, 3, 5, 6, 27, 30, and 31 of the '149 patent.

27. INSIDE has sold and offered for sale and continues to sell and offer for sale within the United States its Core software tool that infringes the '149 Patent.

28. On information and belief, Synopsys, Inc., has used and continues to use within the United States INSIDE's Core software tool supplied by INSIDE to modify and protect its software application programs from unauthorized copying, modification, tampering, and/or distribution that infringes the '149 Patent.

29. On information and belief, Synopsys, Inc., has imported and continues to import into the United States software that has been modified by the method used by INSIDE's Core software tool that infringes the '149 Patent.

COUNT I

(Infringement of the '149 Patent)

30. The allegations of paragraphs 1 to 29 are incorporated herein by reference.

31. The '149 Patent, entitled "Method for Runtime Code Integrity Validation Using Code Block Checksums" was duly and legally issued by the United States Patent and Trademark Office ("USPTO") on April 12, 2005. PACE is the sole and exclusive owner of the '149 Patent.

32. INSIDE, without authority or consent from PACE, has sold and offered for sale, and continue to sell and offer for sale, in the United States products that infringe the '149 Patent, either literally or under the doctrine of equivalents, by making, using, selling, offering to sell, and/or importing into the United States software products including but not limited to the Core product ("Accused Product"). As set forth below, the Accused Product infringes at least claims 1, 2, 3, 5, 6, 27, 30, and 31 of the '149 Patent. For exemplary purposes, the Accused Product will demonstrate infringement of each method step of Claim 1 below.

33. Claim 1 of the '149 patent recites as follows:

> 1. A method for performing runtime checksum validation of a software program, the method comprising the steps of:
>
> (a) providing a software tool as well as instructions on how to modify the software program to submit to the tool, wherein executable code is generated from the modified software program that includes checksum information for the tool to use when processing the software program;

/ / /

/ / /

> (b) in response to the executable code being submitted to the tool, the tool calculates at least one checksum, embeds the checksum in the executable code in a location indicated by the checksum information, and strips the checksum information from the executable code; and
>
> (c) delivering the executable code as a protected software program, wherein during execution, the protected software application generates a new checksum and determines that the software application has been modified if the new checksum fails to match the embedded checksum.

34. INSIDE's Accused Product meets all requirements of claim 1. On information and belief, the Accused Products perform a method that includes providing a software tool as well as instructions on how to modify the software program to submit to the tool, wherein executable code is generated from the modified software program that includes checksum information for the tool to use when processing the software program. Modules that are a part of the Accused Product such as, for example, MFDBExtract, MFDBLink, MFDBmerge, MFDButil, MFFixup, MFInjector, MFProfiler, and MFView are provided by INSIDE to a customer seeking to protect its software application programs from unauthorized copying, modification, tampering, and/or distribution. One example is the MFInjector module which, on information and belief, performs protection injections at the source code level (e.g., adding the checksum data, the checksum loop, and response code). Another example is the MFFixup module which operates on the linked executable to compute the checksum zones, checksum algorithms, and then embeds the computed checksums and zones into the binary so that the checksum values can be verified at runtime.

35. The Accused Product performs a method that includes the tool calculating at least one checksum, embedding the checksum in the executable code in a location indicated by the checksum information, and stripping the checksum information from the executable code. On information and belief, the Accused Product obtains a checksum value by using its own checksum algorithm, embeds the checksum value directly into the executable code, and then copies the checksum value to a local stack variable with an offset of -0x1cc (hex value). On information and belief, this local copy of the checksum value on the stack is then used throughout the rest of the injected security code.

/ / /

36. The Accused Products perform a method that includes delivering the executable code as a protected software program, wherein during execution, the protected software application generates a new checksum and determines that the software application has been modified if the new checksum fails to match the embedded checksum. On information and belief, the Accused Product integrates directly into the customer's software build, automatically converting software programs to protected software programs. On information and belief, the resulting executable of the protected software program includes instructions to determine checksum values at runtime and compare the runtime checksum values with the embedded checksum value. On information and belief, when the compared checksum values match, the program follows the "good path" in the code and the protected code able to continue to run for the end user. Alternatively, on information and belief, when the compared checksum values fail to match, the program enters the "bad path" in the code and an error is encountered, rendering the protected code inoperable.

37. INSIDE's continuing infringement of the '149 patent will continue to damage PACE, causing irreparable harm for which there is no adequate remedy at law, unless INSIDE is enjoined by this Court from further acts of infringement.

38. INSIDE's past and future acts of infringement of the '149 patent have caused and will cause damages to PACE, entitling PACE to recover damages from INSIDE in an amount subject to proof at trial, but in no event less than a reasonable royalty extending through the life of the '149 patent.

RELIEF SOUGHT

WHEREFORE, Plaintiff respectfully requests that the Court enter a judgment against INSIDE as follows:

1. A judgment that INSIDE has infringed the '149 Patent;

/ / /

/ / /

/ / /

/ / /

2. A order preliminarily and permanently enjoining INSIDE and its officers, directors, employees, agents, licensees, representatives, affiliates, related companies, successors, and assigns, and any and all persons acting in privity or in concert with any of them, from further infringing the '149 Patent. In the alternative, if the Court finds that an injunction is not warranted, PACE requests an award of post-judgment royalty to compensate for future infringement;

3. An award of damages together with prejudgment and post-judgment pursuant to 35 U.S.C. § 284 in an amount to be determined at trial, as a result of INSIDE's infringement of the '149 Patent;

4. For an order finding that this is an exceptional case under 35 U.S.C. § 285 and awarding relief, including reasonable attorneys' fees, costs, and expenses; and

5. For such other and further relief as this Court may deem proper and just.

DEMAND FOR JURY TRIAL

PACE hereby demands a trial by jury on all issues so triable.

Dated: October 12, 2017

HOPKINS & CARLEY
A Law Corporation

By: */s/ John V. Picone III*
John V. Picone III
Jennifer S. Coleman
C. Gideon Korrell
Attorneys for Plaintiff
PACE Anti-Piracy, Inc.